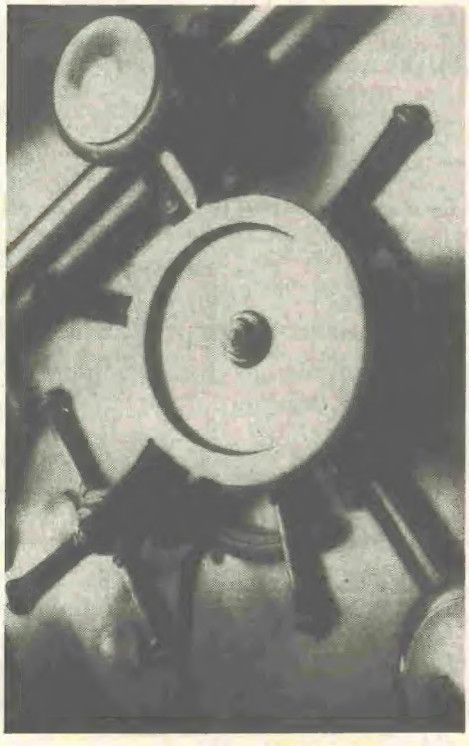
สหัส พรหมสิทธิ์

ใช้ SATAN อุดช่องโหว่ในอินเทอร์เน็ต

SATAN มีจุดมุ่งหมาย ทำหน้าที่เป็นโปรแกรม สืบสวนที่เป็นแบบอัตโนมัติ



เน็ตเวอร์กสากลเช่นกรณีของอินเทอร์เน็ต ย่อมให้ทั้งคุณประโยชน์ในแง่ของการใช้เพื่อแลกเปลี่ยนข้อมูล ใช้ในการประชาสัมพันธ์หรือการค้าบนฐานอิเล็กทรอนิกส์ แต่ในท่ามกลางประโยชน์อย่างอเนกอนันต์ของอินเทอร์เน็ตก็จะตามมาด้วยปัญหาในเรื่องของภยันตรายต่าง ๆ ที่เกิดจากช่องโหว่ของอินเทอร์เน็ต รวมทั้งที่เกิดจากการกระทำของโปรแกรมเมอร์สมัครเล่นที่มีความอยากรู้อยากเห็นไปเสียทุกเรื่องว่าในเวบไซท์ที่กระจายอยู่ทั่วโลกนั้นมีกิจกรรมอะไรบ้างที่สามารถเรียกร้องความสนใจจนน่าเข้าไปทำการสอดแนมหรือเคาะประตูเพื่อขอเข้าไปดูว่าใครกำลังทำอะไรอยู่ อันเป็นการบุกรุกที่มีทั้งการทำไปด้วยความอยากรู้ รวมทั้งเพื่อการโจรกรรม หรือเพื่อสร้างความเสียหายให้แก่ข้อมูลที่เป็นทั้งของภาครัฐและเอกชน ทำให้เกิดมีผู้ที่มีความปรารถนาดีต้องออกมาปกป้องภยันตรายต่าง ๆ ที่จะมีกับอินเทอร์เน็ต เช่น กรณีของนายแดน ฟาร์มเมอร์ (Dan Farmer) ซึ่งเป็นหนึ่งในปรมาจารย์ในด้านการเขียนโปรแกรมที่ไม่อยากเห็นอินเทอร์เน็ตถูกพวกมือบอนหรือพวกมิจฉาชีพบุกรุกย่ำยี จนทำให้เกิดผลกระทบในแง่ของความเสียหายกับกิจการต่าง ๆ อันนับตั้งแต่อาทิเช่น เรื่องของธนาคาร งานด้านบัตรเครดิต หน่วยงานของรัฐ ธุรกิจการค้าที่อาศัยกลไกทางอิเล็กทรอนิกส์ (Electronic Commerce) จนถึงเวบไซท์อีกมากมายหลายแห่งที่มีโอกาสถูกจู่โจมหากไม่มีมาตรการในการป้องกันที่รัดกุม ทำให้เกิดมีโปรแกรมที่ทำหน้าที่เป็นนักสืบขึ้นมาในชื่อว่า SATAN (Security Administrator Tool for Analyging Networks) ซึ่งมีนายแดน ฟาร์มเมอร์เป็นผู้ร่วมพัฒนาโปรแกรมตัวนี้ โดยมีจุดมุ่งหมายให้ทำหน้าที่เป็นโปรแกรมสืบสวนที่เป็นแบบอัตโนมัติ (Automated Investigative Program)

สรรพสัตว์ในอินเทอร์เน็ต

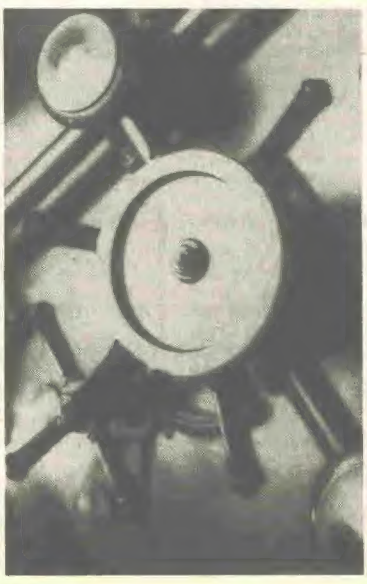
การทำงานของ SATAN จะอาศัยหลักการในรูปของการย่องเบา (hacking tricks) เข้าไปในอินเทอร์เน็ตไซท์ โดยไม่จำเป็นต้องเข้าไปในฐานะของการพังประตูหรือทำลายหน้าต่างแต่อย่างใด ความใจกว้างหวังดีของ

นายแดน ฟาร์มเมอร์ยังมีต่อไปอีก ด้วยการแจกโปรแกรม SATAN ให้เป็นของสาธารณะในท่ามกลางที่มีผู้วิจารณ์กันอย่างหนาหู เนื่องจากว่าอาจมีผู้ใช้โปรแกรมนี้ในการวิ่งสำรวจไปตามไซท์ต่าง ๆ เพื่อหาโอกาสบุกรุกจู่โจมได้โดยไม่ต้องลงทุนลงแรง อย่างไรก็ตาม การกระทำของนายแดน ฟาร์มเมอร์ก็ยังคงถือได้ว่ามีความห่วงใยต่อสาธารณะ ด้วยการแจ้งเตือนให้ผู้ที่ใช้อินเทอร์เน็ตเพื่อให้บริการต่าง ๆ ได้รู้ว่ายังมีอีกหลายแห่งที่ซีเคียวริตี้ยังอยู่ในระดับต่ำ SATAN จึงน่าจะให้คุณในแง่ของการกระตุ้นให้ผู้ที่เกี่ยวข้องกับอินเทอร์เน็ตได้รู้ถึงภัยเสี่ยงต่าง ๆ ที่อาจก่อให้เกิดปัญหาใหม่ ๆ ที่ยากแก่การแก้ไข

ถ้าหากจะถามว่าการมีอุปกรณ์ตรวจสอบการเสี่ยงในอินเทอร์เน็ตเช่น SATAN แล้วจะทำให้เน็ตมีความปลอดภัยมากขึ้นหรือไม่ คำตอบก็คือ ยังห่างไกลจากความปลอดภัยอย่างมาก เนื่องจากว่าแต่ก่อนนั้นถ้าใครสักคนเดินทางในเน็ตเพื่อไปเยี่ยมเวบไซท์แห่งใดแห่งหนึ่ง ก็จะใช้ browser เป็นเครื่องมือในการอ่านเนื้อหาหรือข้อมูลที่มีไว้ให้ผู้สนใจในเรื่องใดเรื่องหนึ่ง อันจะผิดกับในปัจจุบันที่ภายในเวบ (Web) เต็มไปด้วยโปรแกรมขนาดเล็กซึ่งจะโหลดตัวของมันเอง เมื่อผู้ใช้เวบเพจและวิ่งโปรแกรมดังกล่าวในเครื่องของตน โปรแกรมขนาดเล็กเหล่านี้อาจได้รับการถ่ายทอดจากผู้เขียนโปรแกรมที่มีเจตนาไม่ดีที่คิดจะสร้างมันขึ้นมาให้ไปก่อปัญหากับผู้อื่น และเมื่อใดที่มันได้มีโอกาสวิ่งเข้าไปในคอมพิวเตอร์ที่โหลดมันเข้าไป ผู้ใช้คอมพิวเตอร์นั้นก็จะตกเป็นเหยื่อที่ถูกก่อกวนจนเกิดความเอือมระอา

นอกจากนี้ก็ยังมีภัยชนิดอื่นที่วิ่งกันพล่านในเน็ตในปัจจุบัน อันหมายถึงการมีประชากรที่ไม่พึงปรารถนาปรากฏออกมากระโดดโลดเต้นกันอย่างสนุก โดยแฝงมาในรูปของสิ่งมีชีวิตขนาดเล็ก เช่น แมงมุม สัตว์ที่คลานได้ หนอน เอเยนต์ รวมทั้งสรรพสัตว์ที่เป็นอัตโนมัติอื่น ๆ ซึ่งได้รับการออกแบบให้ทำการแทรกซึมเวบไซท์ต่าง ๆ เพื่อค้นหาข้อมูลที่เป็นของหวงห้ามจากแต่ละไซท์ โปรแกรมเล็ก ๆ เช่นนี้จึงเป็นเสมือนเครื่องมืออันวิเศษสำหรับผู้มองสังคมในแง่ร้ายที่มักฉวยโอกาสรุกล้ำเข้าไปในไซท์ที่มีจุดอ่อนป้องกันตนเองไม่ได้ เพื่อไปทำอันตราย แต่ถ้าจะมองในแง่ดีก็น่าจะเป็นว่าอินเทอร์เน็ตยังคงเป็นสังคมที่เกือบไม่มีอาชญากรที่มีขนาดใหญ่ที่สุดในโลก เนื่องจากว่าอาชญากรที่เรียกว่า **แฮกเกอร์** (hackers) ยังคงมีความซื่อสัตย์ที่เป็นพื้นฐานของนิสัยของพลเมืองดีอยู่พอสมควรในท่ามกลางของการรักษาความปลอดภัยในเน็ตที่ยังไม่มีการเข้มงวดในเรื่องการปิดล็อก สำหรับในอีกหลาย ๆ ไซท์ หรืออาจยังไม่มีอะไรในเน็ตให้ทำการโจรกรรมที่เป็นชิ้นเป็นอัน เว้นแต่ว่าผู้ที่คิดจะกระทำการร้ายในเน็ตจะทำไปเพื่อแก้แค้นผู้ที่เป็นศัตรู

อย่างไรก็ตาม เรื่องของซีเคียวริตี้ในเน็ตจะเป็นเรื่องใหญ่ที่มีความสำคัญเป็นอันดับหนึ่ง เพราะการใช้เน็ตในปัจจุบันและต่อไปจะมีเรื่องของการค้าเข้ามาเกี่ยวข้องมากขึ้นเรื่อย ๆ การป้องกันเพื่อไม่ให้มีการโจรกรรมข้อมูลข่าวสารในแง่ของการมีรั้วรอบขอบชิดรวมทั้งการทำให้ประตูและหน้าต่างทุกบานสามารถปิดได้อย่างสนิท จึงมีความสำคัญกว่าเรื่องอื่น ๆ ทำให้มีการสำรวจความล่อแหลมโดยอาศัยเครื่องมือในรูปของผู้จัดการด้านซีเคียว-ริตี้ที่ทำหน้าที่วิเคราะห์ความปลอดภัยในเน็ตเวอร์กเช่นกรณีของ SATAN



วีรกรรมของ SATAN

หน้าที่ของ SATAN ก็คือการสำรวจคอมพิวเตอร์เน็ตเวอร์กเพื่อดูว่ามีความปลอดภัยจากการแทรกแซงรบกวนจากผู้ไม่ประสงค์ดีหรือไม่ การสำรวจของ SATAN เป็นไปอย่างอัตโนมัติเหมือนนักสำรวจที่เป็นมนุษย์ อันเนื่องจากมีความพร้อมในแง่ของการเป็นซอฟต์แวร์ชั้นดีว่า จะทำการสำรวจอะไรบ้างในไซท์ต่าง ๆ ที่ได้รับคำสั่งให้ไปสำรวจโดย **อาศัยวิจารณญาณ**ที่ผู้เขียนซอฟต์แวร์เป็นผู้สร้างสรรค์ การใช้วิจารณญาณในทำนองนี้คงหนีไม่พ้นการใช้วิทยาการด้าน AI (Artificial Intelligence) เข้าช่วย เพื่อให้ซอฟต์แวร์สามารถมองปัญหาและคิดหาวิธีการแก้ปัญหาได้อย่างฉลาดเหมือนมนุษย์ การใช้ SATAN ในขั้นแรกได้หนักไปในการสำรวจอย่างกว้าง ๆ สำหรับไซท์ต่าง ๆ ในเวิร์ลไวด์เวบ รวมทั้งไซท์ที่เป็นการค้า ซึ่งก็ได้ผลออกมาว่าได้มีอยู่หลายแห่งที่ล่อแหลมต่อการถูกโจรกรรมหรือถูกบิดเบือนปลอมแปลงข้อมูล

แหล่งหรือไซท์ที่น่าจะอันตรายมาก ๆ ก็คือที่ที่ต้องการให้ลูกค้าแจ้งรายละเอียดในบัตรเครดิตเมื่อต้องการสั่งสินค้าหรือใช้บริการต่าง ๆ อันเป็นการเปิดโอกาสให้ผู้ไม่ประสงค์ดีที่แฝงเร้นมาในเน็ตสามารถคัดลอกข้อมูลในบัตรเครดิต (ของผู้ซื้อสินค้าหรือผู้ใช้บริการ) แล้วนำไปใช้ในทางทุจริตได้อย่างสบาย งานสำรวจอีกส่วนหนึ่งของ SATAN จะหนักไปในการเก็บข้อมูลว่าได้มี**ปัญหาในด้านซีเคียว-ริตี้**อะไรบ้างในขณะนี้ซึ่งเป็นที่รู้กันอย่างแพร่หลาย ซึ่งรวมถึงไฟล์เก็บชื่อรหัส (password files) ต่าง ๆ ที่นำมาดาวน์โหลดได้โดยใช้โปรโตคอลมาตรฐานเช่น File Transfer Protocol รวมทั้งโปรแกรมอีกตัวหนึ่งซึ่งเป็นเหมือนคาบสองคมที่มีชื่อว่า Sendmail ที่เปิดโอกาสให้บรรดานักย่องเบาสามารถใช้เป็นพาหะในการส่งโปรแกรมต่าง ๆ เข้าไปในระบบคอมพิวเตอร์ที่เป็นของแต่ละไซท์ โปรแกรมต่าง ๆ ดังกล่าวมีทั้งที่เขียนขึ้นมาด้วยความอยากรู้อยากเห็นความเป็นไปในเน็ตโดยเฉพาะตามไซท์ต่าง ๆ โดยผู้เขียนโปรแกรมไม่มีความ

ช่องโหว่ในอินเทอร์เน็ต			
ประเภทของเวบไซท์	จำนวนโฮสต์ที่ได้รับการสแกน	ภยันตราย คิดเป็นร้อยละ	ปัญหาด้านซีเคียวริตี้ (security) คิดเป็นร้อยละ
ธนาคาร	660	68.33	35.61
เครดิต-ยูเนียน	274	51.09	20.44
รัฐบาลสหรัฐฯ	47	61.70	38.30
หนังสือพิมพ์	312	69.55	38.78
การค้าด้วยอิเล็กทรอนิกส์	451	66.08	25.50
สุ่ม (random) จากจุดต่าง ๆ	469	33.05	17.27

ตารางที่ 1 แสดงความล่อแหลมของไซท์ต่าง ๆ ในเน็ต ซึ่งกว่าร้อยละ 60 ของจำนวนไซท์อาจถูกจู่โจมได้โดยง่าย รวมทั้งปัญหาต่าง ๆ ในแง่ของซีเคียวริตี้

มุ่งร้าย รวมทั้งโปรแกรมที่เขียนขึ้นมาด้วยจุดประสงค์ร้ายของบรรดามิจฉาชีพ

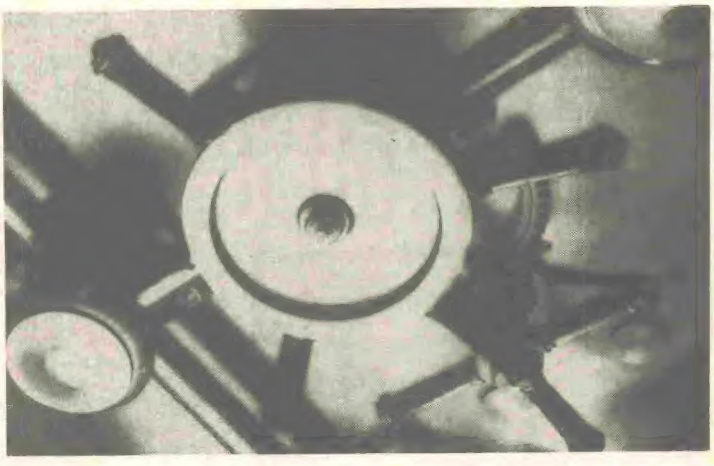
ปรัชญาการออกแบบ SATAN ของทีมงานที่มีอาชีพด้านการให้คำปรึกษาด้านคอมพิวเตอร์ซีเคียวริตี้ ซึ่งตั้งอยู่ที่เบิร์กเลย์ แคลิฟอร์เนีย (โดยมีนายแดน ฟาร์มเมอร์เป็นหนึ่งในทีม) มีว่า SATAN ควรเป็นโปรแกรมที่ทำให้ผู้บริหารระบบคอมพิวเตอร์สามารถค้นหารูรั่วต่าง ๆ ในด้านซีเคียวริตี้ที่ปรากฏในเน็ตเวอร์กของแต่ละห้างร้านหรือแต่ละวิสาหกิจ ต่อมาก็ได้มีการแจกโปรแกรมนี้ด้วยการปิดประกาศไว้ในอินเทอร์เน็ตในเดือนเมษายน 1995 เพื่อให้ผู้สนใจสามารถที่จะดาวน์โหลดโปรแกรมนี้ไว้ใช้ในคอมพิวเตอร์ของตน ซึ่งก็มีเสียงคัดค้าน เพราะมีผู้เกรงว่าบรรดานักตัดช่องย่องเบาจะได้ระแคะระคายและไปทำอันตรายให้แก่อินเทอร์เน็ตไซท์ต่าง ๆ ที่ SATAN เป็นผู้เปิดโปงว่ามีจุดอ่อน การปล่อย SATAN ให้เป็นสมบัติสาธารณะนี้ได้ส่งผลให้เกิดมีการตรวจสอบซีเคียวริตี้ของคอมพิวเตอร์เน็ตเวอร์กต่าง ๆ ที่กระจายอยู่ทั่วโลกเป็นการใหญ่ พร้อมด้วยการพัฒนาโปรแกรมขึ้นมาอีกหลายตัวเพื่อคอยติดตามการเคลื่อนไหวของ SATAN

ฟาร์มเมอร์ได้พบว่า การต่อต้าน SATAN ของผู้เป็นเจ้าของคอมพิวเตอร์เน็ตเวอร์กและระบบคอมพิวเตอร์หลาย ๆ แห่งนั้นไม่ได้มีส่วนปรับปรุงให้ซีเคียวริตี้ในอินเทอร์เน็ตดีขึ้นเลย ดังจะเห็นได้จากการที่ฟาร์มเมอร์ได้ใช้ SATAN ในการทำการสำรวจโดยไม่ขออนุญาตเข้าไปในเวบไซท์จำนวนกว่า 2,200 แห่งในระหว่างเดือนพฤศจิกายนและธันวาคมของปี 1996 โดยอาศัยรายชื่อที่ประมวลโดย Yahoo ที่เรียกว่า Internet Indexing Service ซึ่งฟาร์มเมอร์ได้เลือกไซท์ต่าง ๆ ที่เป็นของธนาคาร เครดิต ยูเนียน รัฐบาลสหรัฐฯ หนังสือพิมพ์ รวมทั้งบริษัทที่ทำการค้าด้วยวิธีการทางอิเล็กทรอนิกส์โดยอาศัยเน็ต โดยมีอยู่หลายแห่งที่ขายภาพอนาจารหรือเปิดโอกาสให้มีการซื้อบริการเพื่อเข้าสู่การดูภาพอนาจาร งานสำรวจของฟาร์มเมอร์ยังรวมถึงการสุ่มเลือกเพื่อทำการตรวจตราไซท์อื่น ๆ แบบอิสระอันนอกเหนือจากที่กล่าวมาในวรรคแรก และได้รวบรวมผลดังแสดงในตารางที่ 1

การสำรวจของฟาร์มเมอร์ด้วย SATAN ทำให้พบว่า กว่าร้อยละ 60 ของไซท์มีช่องโหว่ที่เปิดโอกาสให้มีการบุกรุกเข้าไปได้ (ดูตารางที่ 1) และกว่าครึ่งหนึ่งของไซท์ดังกล่าวจะมีปัญหาในด้านซีเคียวริตี้ ทำให้นักย่องเบาที่มีฝีมือสามารถทำลายหรือก่อการร้ายแก่ข้อมูลข่าวสารที่อยู่ในโฮสต์คอมพิวเตอร์ ฟาร์มเมอร์ได้ให้ความเห็นว่า ความรู้ในเรื่องของช่องโหว่ทางซีเคียวริตี้เท่าที่พูดมานี้ไม่ใช่ของใหม่ จุดอ่อนต่าง ๆ ที่ SATAN ได้ค้นหานั้นได้มีการประกาศเวียนให้รู้กันอยู่แล้ว ด้วยความอนุเคราะห์ของหน่วยงานหรือองค์กรที่สนใจในด้านคอมพิวเตอร์ซีเคียวริตี้ ซึ่งมีอาทิเช่น The Computer Emergency Response Team อันเป็นองค์การที่คอยเก็บข้อมูลที่เกี่ยวกับช่องโหว่ทางซีเคียวริตี้ในโปรแกรมที่ใช้ในเชิงพาณิชย์

สิ่งที่ฟาร์มเมอร์เป็นห่วงมากที่สุดก็คือข้อเปิดเผยที่ว่าไซท์ต่าง ๆ ที่เป็นของธนาคาร หน่วยงานของรัฐบาล และบริษัทต่าง ๆ ที่ขายบริการผ่านอินเทอร์เน็ตนั้นมีอันตรายมากกว่าไซท์ที่ได้รับการสำรวจแบบสุ่มตัวอย่าง (random) random sites ที่ได้รับการตรวจสอบโดยฟาร์มเมอร์มีปัญหาเพียงครึ่งหนึ่งของไซท์ต่าง ๆ ที่มีระบบที่มีสภาพเป็น critical systems ซึ่งในจำนวนทั้งหมดก็มีอยู่เพียง 3 แห่งที่สามารถล่วงรู้ว่า SATAN ได้ย่างกรายมาเคาะประตูและทุบหน้าต่าง ฟาร์มเมอร์มีความเชื่อว่าแหล่งอันเป็นไซท์ทางการค้ารวมทั้งแหล่งอื่น ๆ ที่เป็นไซท์ขนาดใหญ่ในอินเทอร์เน็ตได้ยอมแลกซีเคียวริตี้กับการพยายามให้บริการทางการค้าชนิดมากมายหลายอย่าง อันจะมีผลว่าถ้าเกิดมีข้อผิดพลาดขึ้นในการจัดเรียงโปรแกรมต่าง ๆ ให้อยู่ในระบบและผิดไปเพียงโปรแกรมเดียวก็จะสามารถทำให้บรรดาประตูและหน้าต่างของไซท์แห่งใดแห่งหนึ่งเปิดอ้าหมดทุกบานได้อย่างสบาย

นอกจากนี้การที่เวบไซท์ของบริษัทใดบริษัทหนึ่งตกอยู่ในภยันตรายก็ไม่ได้หมายความว่า ระบบคอมพิวเตอร์ทั้งระบบจะต้องมีอันตรายจากการถูกจู่โจม เช่นในกรณีของธนาคารที่มีการระวังไม่ให้ระบบคอมพิวเตอร์ที่มีหน้าที่ดูแลบัญชีของลูกค้าไปปะปนกับระบบคอมพิวเตอร์ที่ต้องเชื่อมโยงกับเน็ตเวอร์กเช่นอินเทอร์เน็ต อย่างไรก็ตาม ในขณะที่อินเทอร์เน็ตนับแต่จะมีบทบาทในโลกของธุรกิจการค้ามากขึ้นทุกวัน ภยันตรายที่เกิดจากการเล็ดลอดและปลอมแปลงก็คงต้องเพิ่มมากขึ้นอย่างหนีไม่พ้น และผู้ที่รับภาระหนักในการป้องกันภยันตรายในด้านนี้คงหนีไม่พ้นผู้เชี่ยวชาญด้านคอมพิวเตอร์เน็ตเวอร์กซีเคียวริตี้ อย่างไรก็ตาม ยังมีพ่อค้าและสมาชิกของเน็ต



บางรายที่ไม่เห็นพ้องกับฟาร์มเมอร์ โดยอ้างว่าคำเตือนของฟาร์มเมอร์ดูน่ากลัว เช่น กรณีของ นายนิค โอคเด็น (Nick Ogden) ซึ่งเป็นผู้จัดการด้านวิจัยและพัฒนาของซุปเปอร์เน็ต (Supernet) อันเป็นบริษัทที่มีสำนักงานใหญ่ที่นิวเจอร์ซี่ ที่ให้บริการในการดำเนินงานให้แก่เวบไซท์สำหรับการซื้อแบบออนไลน์ เช่น ศูนย์การค้า Bardays Square ได้โต้แย้งว่า ไซท์อันเป็นที่ตั้งของ Bardays Square ซึ่งไม่ได้รับการสำรวจจากฟาร์มเมอร์ ได้รับการเยี่ยมเยียนจากลูกค้ากว่า 300,000 รายต่อเดือน โดยมีลูกค้าหลายรายที่ซื้อสินค้าด้วยบัตรเครดิต โอคเด็นได้ให้ข้อคิดเห็นว่า "ถ้าลูกค้าที่มาซื้อของได้ใช้บัตรเครดิต แล้วถูกล้วงความลับของข้อมูลที่อยู่ในบัตร ก็คงไม่กลับมาซื้อของที่ Bardays Square อีกแน่ ๆ

ซีเคียวริตี้ในวงกว้าง

เมื่อพูดถึงเรื่องราวของคอมพิวเตอร์ซีเคียวริตี้ในเน็ตที่เกี่ยวกับความปลอดภัยของเวบไซท์ต่าง ๆ แล้ว ก็อยากพูดถึงหน่วยงานหนึ่งในสหรัฐฯ ซึ่งเป็นที่ยอมรับกันว่ามีความรู้ในเรื่องคอมพิวเตอร์ซีเคียวริตี้อย่างทะลุปรุโปร่ง ภายใต้ชื่อว่า The National Computer Security Association (NCSA) ซึ่งก่อตั้งเมื่อปี 1989 ขอบข่ายความรับผิดชอบตลอดจนผลงานของ NCSA มีมากมาย ทั้งในด้านของการตีพิมพ์เพื่อเผยแพร่ความรู้ในด้านซีเคียวริตี้ อาทิเช่น เรื่องของ firewalls, cucryption และอื่น ๆ ที่เกี่ยวกับโลกของซีเคียวริตี้ รวมทั้งการให้บริการในด้านการฝึกอบรมและให้คำปรึกษาในเรื่องของคอมพิวเตอร์ซีเคียวริตี้ ที่สำคัญที่สุดก็คือการมีทีมงานที่สามารถดักซุ่มเพื่อคอยดูการจู่โจมเข้ามาในเน็ตเวอร์ก โดยสามารถบอกให้ลูกค้าหรือผู้ที่มาใช้บริการของ NCSA ให้รู้ว่า มีใครบ้างที่กำลังจะแกะรอยเข้ามาในเน็ตเวอร์กของผู้เป็นลูกค้าและจะเข้ามาทางช่องโหว่ไหนบ้าง

ภาระสำคัญอีกประการของ NCSA ก็คือการจัดให้มีการประชุมใหญ่ทางวิชาการ (conferences) อย่างบ่อยครั้ง เช่น การประชุมที่เรียกว่า CyberRisk โดยมีสถาบันที่มีชื่อว่า The Computer Ethics Institute เป็นผู้ร่วมอุปถัมภ์ เช่นเมื่อคราวที่แล้วก็ได้มีการประชุมเมื่อ 7-8 พ.ย. 96 ที่กรุงวอชิงตัน ดี.ซี. แนวคิดในการจัดให้มีการประชุมใหญ่ที่เรียกว่า CyberRisk เป็นของใหม่อีกอันที่ NCSA ริเริ่มขึ้นเมื่อเร็ว ๆ นี้ โดยมีจุดมุ่งหมายที่จะให้ผู้ใช้เน็ตเวอร์กทั้งหลายรักษามารยาทในการสื่อสารด้วยคอมพิวเตอร์เน็ตเวอร์กเช่นกรณีของอินเทอร์เน็ตว่าความพอเหมาะพอดีอยู่ตรงไหน เช่นในแง่ของการครอบครอง การสงวนความลับส่วนบุคคล privacy คืออะไร ฯลฯ ซึ่งถ้าจะยกตัวอย่างในเรื่องนี้ก็จะมีอาทิเช่น sysops ควรรายงานเรื่องที่ใครเป็นผู้อ่านข้อมูลในเวบไซท์ไหนเพื่อให้ผู้บริหารรับทราบ ใครเป็นผู้ครอบครองเวบเพจส่วนบุคคลที่อาศัยเซอร์ฟเวอร์ของบริษัท การติดตามอ่านอีเมล์ของพนักงานเป็นการละเมิดสิทธิส่วนบุคคลหรือไม่ privacy คืออะไร ฯลฯ อันเป็นนโยบายในการบริหารบริษัทหรือวิสาหกิจที่ยังไม่มีความชัดเจน และ CyberRisk เห็นว่าควรนำมาถกเถียงเพื่อหาข้อยุติในการประชุมแบบ conference

หัวข้อในการประชุม CyberRisk ที่จัดขึ้นเมื่อเร็ว ๆ นี้ (7-8 พ.ย. 96) ประกอบด้วย

- มารยาทในเรื่องของ penetration analysis (เช่น เมื่อบริษัทได้ว่าจ้างผู้เชี่ยวชาญด้านซีเคียวริตี้จากภายนอกให้มาทดสอบความพร้อมของเน็ตเวอร์กของบริษัทในการป้องกันการจู่โจมจากมิจฉาชีพ ในกรณีนี้ผู้เชี่ยวชาญควรอาศัยจรรยาบรรณอะไรบ้างในการทดสอบเพื่อจู่โจมเข้าไปในเน็ตเวอร์กของลูกค้าอย่างถูกหลักวิชา) องค์ปาฐกถาคือ Ira Winkler ซึ่งเป็นผู้อำนวยการด้านเทคโนโลยีของ NCSA
- ว่าด้วยจรรยาบรรณสำหรับการตลาดแบบออนไลน์ โดยมีองค์ปาฐกถาชื่อ Mich Kabay ผู้ทำหน้าที่ผู้อำนวยการด้านฝึกอบรมของ NCSA
- autonomous agents ซึ่งปาฐกถาโดย Ramone Barquin จาก Computer Ethics Institute

การจัดประชุมเชิงวิชาการที่เรียกว่า CyberRisk นี้เป็นส่วนหนึ่งของการรณรงค์ในระดับชาติที่ว่าด้วยจรรยาบรรณในการใช้คอมพิวเตอร์ในคอมพิวเตอร์เน็ตเวอร์ก อันเป็นการรณรงค์ในเรื่องของความรับผิดชอบซึ่งกำลังจะมีความสำคัญมากขึ้นทุกที ช่องว่างที่การประชุม CyberRisk พยายามจะเข้าไปอุดสำหรับในขณะนี้ก็คือเรื่องที่ไม่ค่อยจะมีใครพูดกันอย่างกว้างขวาง และยังเป็นเรื่องที่ขาดความเด่นชัดในทางปฏิบัติ โดยเฉพาะแง่ของการกำหนดนโยบายของธุรกิจหรือวิสาหกิจ (corporate policy) การประชุมทำนองนี้จึงมีเรื่องของกฎหมายรัฐธรรมนูญในวงกว้าง (broad constitutional theories) เข้ามาเกี่ยวข้องรวมทั้งสิทธิมนุษยชนที่เรียกว่า First Amendment ที่ต้องนำมาถกกันในที่ประชุม เพื่อให้ CyberRisk มีความสมบูรณ์ในทุกแง่มุม โดยเฉพาะในทางปฏิบัติ

จากนี้ก็จะขอพูดถึงโปรแกรมอื่นที่มีคุณสมบัติในการสืบสวนเหมือน SATAN ว่ามีอะไรบ้าง

โปรแกรมอื่นนอกเหนือจาก SATAN

โปรแกรมต่าง ๆ เช่น ISS (The Internet Security Scanner) Icepick และ SATAN จะทำงานโดยอาศัยหลักการของการตีผนัง เคาะประตู และหรือทุบหน้าต่าง มาใช้ในการตรวจสอบความมั่นคงปลอดภัยของแต่ละไซท์ เช่นในกรณีของ SATAN ซึ่งสามารถสแกนระบบคอมพิวเตอร์นับเป็นร้อยระบบได้อย่างรวดเร็ว โดยจะมุ่งการตรวจสอบไปที่ปัญหาหรือภัยที่มักจะเกิดบ่อย ๆ เช่น ปัญหาที่ว่าผู้ใช้จากภายนอกจะสามารถเขียนไฟล์ใหม่ (re-write) ใน ftp ไดเรคทอรีได้หรือไม่ เวอร์ชันของ sendmail ที่กำลังใช้อยู่นั้นเป็นรุ่นเก่าที่ยังมี bugs อยู่หรือไม่ ผู้ใช้จากภายนอกสามารถที่จะเข้ามายึด password file ได้หรือไม่ เป็นต้น

ความดีของโปรแกรมเหล่านี้คือการสามารถที่จะแสดงให้ผู้บริหารคอมพิวเตอร์เน็ตเวอร์กมองเห็นช่องโหว่ในระบบคอมพิวเตอร์ของตน แต่สำหรับแฮกเกอร์ที่ฉลาด อุปกรณ์เช่น SATAN ก็จะกลายเป็นเครื่องมือที่ช่วยในการจู่โจมหรือโจรกรรมได้อย่างเป็นเลิศ คือทันทีที่ได้มีการปล่อย SATAN ให้เป็นอิสระในอินเทอร์เน็ตเมื่อเมษายน 1994 ก็มีผลทำให้ผู้บริหารระบบที่กระจายอยู่ทั่วโลกต้องหันมารีบเร่งดำเนินการป้องกัน SATAN ด้วยการอุดรูรั่วในด้านซีเคียวริตี้ อัพเดตซอฟต์แวร์ และเปลี่ยนพาสเวิร์ด กันเป็นการใหญ่ สำหรับในกรณีของวิสาหกิจใหญ่ ๆ บางแห่งก็ทำการต่อต้านอย่างฉับพลันด้วยเครื่องสะกดรอย SATAN ในรูปของซอฟต์แวร์แบบต่าง ๆ (รวมทั้งที่มีชื่อว่า "Gabriel") หน้าที่ของซอฟต์แวร์ต่อต้านที่วิสาหกิจขนาดใหญ่นำออกใช้ก็จะเป็นการรายงานพฤติภาพอันไม่ชอบมาพากลของ SATAN ในขณะเมื่อโปรแกรมตัวนี้ได้แสดงความอยากรู้อยากเห็นด้วยการยิงข้อสงสัยแบบเคาะประตูหรือทางหน้าต่างในเชิงทักทายออกมาทีเดียวเป็นตับ อันเป็นสัญญาณที่ไม่สู้ดีนักสำหรับผู้มีหน้าที่ดูแลและรักษาความปลอดภัยให้แก่ระบบคอมพิวเตอร์ของตน

การป้องกัน

การป้องกันการบุกรุกจู่โจมธุรกิจที่เกี่ยวกับการให้บริการด้วยเน็ตเวอร์กสามารถทำได้หลายทาง เช่น การอำพรางการให้บริการที่มีอยู่เดิมด้วยการเสริมบริการใหม่ ๆ เข้าไปเพื่อให้การบุกรุกเน็ตเวอร์กทำได้ยากยิ่งขึ้น เพราะผู้บุกรุกต้องมีการแสดงตัวเองว่าใครเป็นใคร (authentication) มากขึ้น ในแง่ที่ว่าต้องผ่านด่านหลายชั้น หรืออาจแก้ไขด้วยการเพิ่มซีเคียวริตี้เข้าไปให้มากขึ้น สำหรับธุรกิจให้บริการที่มีอยู่เดิม ตลอดจนการสร้างหลุมพราง (traps) เพื่อให้ผู้บุกรุกเกิดความพยายามที่จะให้เข้ามาใช้บริการ ทำให้จำเป็นต้องมีการทดลองเคาะประตูหรือเขย่าหน้าต่างแบบซ้ำแล้วซ้ำเล่าจนทำให้ผู้ให้บริการรู้ตัวและป้องกันหรือทำการจับกุมได้ทัน

การจู่โจมเน็ตเวอร์กในยุคปัจจุบันยังมีกรรมวิธีอื่น ๆ อีกมาก นับตั้งแต่การใช้วิธีการอย่างง่าย ๆ ไปจนถึงแบบที่ซับซ้อน เช่น **combined attacks** ซึ่งผู้บุกรุกสามารถควบคุมความเป็นไปในเน็ตเวอร์ก โดยอาศัย **network control file** ที่ไม่ค่อยมีใครใช้ โดย **control file** ตัวนี้จะบังคับให้คอมพิวเตอร์ที่อยู่ในเน็ตเวอร์กต้องรับคำสั่งจากผู้บุกรุกแต่เพียงผู้เดียว คำสั่งจากผู้บุกรุกนี้จะเป็นไปในรูปที่ว่ามีอะไรบ้างที่น่าจะทดลองล้วงลูกจากระบบคอมพิวเตอร์ของท่านหรือของบริษัท รวมทั้งการออกคำสั่งให้ส่งผลที่ได้จากการล้วงลูกผ่านทาง e-mail เพื่อไปให้ผู้บุกรุก แม้ว่าบางบริษัทจะมี firewalls คอยระมัดระวังอยู่ก็ตาม จึงจำเป็นต้องอธิบายต่อไปว่า

firewalls ที่อยู่ในเน็ตเวอร์กเกตเวย์ที่จะเชื่อมเข้าสู่อินเทอร์เน็ตในสมัยนี้ไม่สามารถหยุดโปรแกรมที่อยู่ในรูปของโปรแกรมที่มีคุณสมบัติในการ control file ได้ โดยโปรแกรมจะสามารถรับคำสั่งต่าง ๆ ที่มาจากไซท์ที่อยู่ไกลออกไป ประการหนึ่งก็คือว่าการออกแบบ firewalls ได้ถือหลักของการป้องกันไม่ให้บุคคลภายนอกรุกล้ำเข้ามาข้างใน แต่ไม่มีการห้ามไม่ให้คนภายในออกไปภายนอก และจะไม่สะกัดกั้น e-mail เนื่องจากว่าการออกแบบ firewalls มักจะยอมให้ e-mail ผ่านออกไปได้ นอกจากจะมีปรัชญาการออกแบบเป็นอย่างอื่น

สรุป

การป้องกันการบุกรุกจู่โจมเข้าไปในระบบคอมพิวเตอร์ที่อยู่ในเน็ตเวอร์กเช่นอินเทอร์เน็ตอาจทำได้ยาก โดยเฉพาะในประเทศที่มีความรุดหน้าทางเทคโนโลยีสูง อันทำให้มีผู้รู้ในด้านนี้มาก แต่ของทุกอย่างในโลกนี้เมื่อมีโจรกรรมได้ก็ต้องมีทางแก้ไขในรูปของหนามยอกเอาหนามบ่ง อันหมายถึงว่านอกจากจะตั้งอยู่ในความไม่ประมาทแล้ว ยังต้องติดตามการรุดหน้าทางเทคโนโลยีอยู่ตลอดเวลา โดยเฉพาะในแง่ของคอมพิวเตอร์ซีเคียวริตี้ ถ้าทำเช่นนี้ได้ก็สามารถป้องกันโจรกรรมได้โดยไม่ยาก